PATHS TO BECOMING A PENETRATION TESTER

Or what I wish I had known when I started out 9 years ago…

WHO AM I…

- Bloomsburg University – Computer Science
- But I have always had an interest in cyber security and hacking
  - Finding ways to make computers do things that they were not meant to do
  - So that we can get the issues fixed before the attackers discover them and try to abuse them
- Dakota State University - Masters in Information Assurance
- GWAPT, GPEN certifications
- My day job is penetration testing for an IT company
- In my free time after work and on weekends, I do security and exploit research

SLIDES

- These slides are available on my Github, so you don't have to try to write down the links
  - https://github.com/koyoresearch

GRAD SCHOOL

- You can do grad school (handy if your employer will pay for it)
- Choose a grad school that aligns with your interest area
  - You can look at the courses the school offers
  - How many (if any) penetration testing courses are offered
    - Some schools do not have any penetration testing courses
    - Some have 1 or 2, or more
- NSA certifies schools for being a Center of Academic Excellence in Cybersecurity
  - CAE-CD: cyber defense
    - Bloomsburg is on this list
  - CAE-CO: cyber operations (more the penetration testing side)

FREE OR LOW COST COURSES

- Cybrary: has many cyber security and penetration testing courses from various authors
  - Many of the courses are free
  - Curated career paths, hands-on virtual labs, and skill assessments are available with their Insider Pro membership, which costs $40/mo
- Portswigger.net/web-security: web app penetration testing training
  - From the creators of the popular Burb Suite web testing tool
  - Free
- Tcm-sec.com: has several penetration testing courses
  - practical ethical hacking; windows privilege escalation; linux privilege escalation; movement, pivoting, and persistence; mobile app pen testing
  - ~$30 per course, with unlimited access to the course once you purchase it

FREE OR LOW COST COURSES

- Udemy.com
  - Search for “penetration testing”
  - ~$15-30 per course
- Linkedin Learning (used to be Linda.com)
  - search for “penetration testing” courses
  - $40/mo or $300/yr ($25/mo) for access to all of the courses
- PentesterLab.com
  - Courses and labs
  - Students: $35 per 3 mo Regular: $20/mo or $200/yr
- PentesterAcademy.com
  - Courses and labs
  - $70/mo, or $250/yr

FREE OR LOW COST COURSES

- Can get certifications from these websites, but their value is meh
  - They might help boost you over another job candidate
  - But they probably won't help to get you through the HR firewall
- They are mostly good for the experience you gain

DECENTLY RESPECTED BUT LOW COST CERTS

- Will get you through the HR firewall
- But don’t require a huge amount of experience
- Certified Ethical Hacker: $1,200 for exam
- CompTia Security+: $380 for exam

OFFENSIVE SECURITY

- Medium cost, but well recognized
- Very in depth training courses, and excellent labs
  - OS / network penetration testing
  - Web application penetration testing
  - etc
- Prepares you for some of the most difficult, but respected certifications in the industry – OSCP, OSWA, etc
  - But even just taking the courses and associated labs will help build your skills tremendously
- They would definitely help boost you over other candidates
  - And get you past the HR firewall
- ~$1000 per course

SANS

- High cost, but well recognized
- In depth training courses, and excellent labs
  - OS / network penetration testing
  - Web application penetration testing
  - etc
- The certifications are not as grueling as the OSCP/OSWA (only 3 hours vs 24 hours), but they are just as well recognized
- They will definitely help boost you over other candidates
  - And get you past the HR firewall
- ~$7,000 for each course
  - But the exams can be taken separately from the courses for ~$1,000
  - And many people do other courses or self study for prep to pass the exams, instead of taking the official courses

LOW COST "LEARN ON YOUR OWN"

- You can also buy textbooks and work through them
  - How I did most of my initial learning
- See what textbooks the college cyber security / penetration testing courses are using
  - From the course descriptions/syllabuses of the colleges in the NSA CAE-CD/CAE-CO list
  - Counter Hack
    - Was written by Ed Skoudis, the original author of Sans' Sec560 penetration testing course. His company also creates the yearly Holiday Hack Challenges.
  - Penetration Testing: A Hands-On Introduction to Hacking
  - etc
- The textbooks usually have guides for setting up a home lab to practice the things taught in the book.

“LEARN ON YOUR OWN” LABS

- You can set up a home lab with intentionally vulnerable systems in a VM and attack them
  - How I did most of my initial learning
- Virtualization options: VirtualBox or VMWare Player free version
  - VirtualBox will allow you to take snapshots, so you can revert to the snapshot when you break something by trying to hack it wrong
  - But you have to have the paid version of VMWare Player to be able to take snapshots
- Kali Linux: a free Linux distro that comes prepackaged with many hacking tools
  - This is commonly used in the industry
  - Parrot OS and Sans’ Slingshot are other alternatives

“LEARN ON YOUR OWN” LABS

- Windows Trials
  - “Free” for 30 days for pc images, 90 days for server images; but you can still use them after they expire
  - https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/
  - https://www.microsoft.com/en-us/evalcenter/
- Prepackaged application stacks; old/vulnerable versions available
  - Turnkey GNU/Linux
  - Ninite.com

“LEARN ON YOUR OWN” LABS

- Can also download trial versions of software that is currently used in the real world
  - And look for vulnerabilities in it
  - This is how the hackers do it
  - Load balancer, firewall software, content management systems, etc
- Can start by walking through an open source version of the software category
  - So you can see how things are usually laid out in the actual source code
  - Before diving into closed source binaries
  - Virtual Box vs VMWare

CAPTURE THE FLAG

- There are many CTFs available online, where you can legally practice your hacking skills, trying to hack in and get the flag
  - Sans holiday hack
  - Hack the box
  - Try hack me
  - Many others, https://www.sans.org/posters/ultimate-pen-test-poster/
- There are also some downloadable CTF packages
  - Metasploitable
  - SecGen (github.com/cliffe/SecGen)
  - Owasp Juicebox
  - Web Goat
- You can also usually find walk-thrus online for the CTFs, guiding you step by step how to do the attacks (how I did a lot of my level-up learning)

BUG BOUNTIES

- Can practice hacking on real world systems via bug bounty programs
  - Hacker One
  - Bug Crowd
  - Etc
- They have lists of companies and their urls that are in scope

AFTER YOU LAND THE JOB

- The learning doesn't stop once you land the job!
- A good penetration tester never stops digging into new stuff and learning, nor do they want to…

IT CAN BE A SLOW START…BUT DON'T GIVE UP

- I started doing IT at an electric utility, and was able to hop over to the cyber security side
  - General cyber security with the occasional penetration test
- I then moved to a banking software company, where I did 50/50 penetration testing and general cyber security
- I then moved to an IT company, where I now do full time penetration testing

QUESTIONS?

- These slides are available on my Github: https://github.com/koyoresearch